UNITED STATES DISTRICT COURT

for the

District of Utah

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

A SAMSUNG CELL PHONE BEARING PHONE NUMBER 970-629-5231, SECURED IN THE EVIDENCE ROOM AT THE GCSO UNDER GCSO 2304793

Case No. 4:23-mj-00164 PK

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A.

located in the _____ District of Utah, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 2422(b)	Coercion and Enticement
18 U.S.C. 2423(b)	Travel with Intent to Engage in Illicit Sexual Conduct

The application is based on these facts:

See attached Affidavit.

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

IVAN J MURRAY Digitally signed by IVAN J MURRAY Date: 2023.09.29 08:09:11 -06'00'

Applicant's signature

HSI Special Agent Ivan Murray

Printed name and title

Sworn to before me and signed in my presence.

Date: 09/29/2023

Judge's signature

City and state: St. George, Utah

United States Magistrate Judge Paul Kohler

Printed name and title

TRINA A. HIGGINS, United States Attorney (#7349)
CHRISTOPHER BURTON, Assistant United States Attorney (NV #12940)
Attorneys for the United States of America
Office of the United States Attorney
20 North Main Street, Suite 208
St. George, Utah 84770
Telephone: (435) 634-4266
Christopher.Burton4@usdoj.gov

IN THE UNITED STATES DISTRICT COURT

DISTRICT OF UTAH

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR A WARRANT AUTHORIZING THE SEARCH OF A SAMSUNG CELL PHONE BEARING PHONE NUMBER 970-629-5231, THAT IS CURRENTLY SECURED IN THE EVIDENCE ROOM AT THE GRAND COUNTY SHERIFF'S OFFICE IN MOAB, UTAH UNDER CASE NUMBER GCSO 2304793	AFFIDAVIT IN SUPPORT OF APPLICATION FOR A SEARCH WARRANT Case No. 4:23-mj-00164 PK

AFFIDAVIT IN SUPPORT OF APPLICATION FOR A SEARCH WARRANT

I, Ivan Murray, Special Agent with Homeland Security Investigations, being duly sworn, state:

AFFIANT BACKGROUND AND QUALIFICATIONS

1. I am a Special Agent with Homeland Security Investigations and have been since November of 2011. I am currently assigned to assist the Federal Bureau of

Investigation's Child Exploitation Task Force (CETF) as well as the Utah Attorney General's Internet Crimes Against Children Task Force (ICAC). Prior to my current position with HSI, I was employed as a Criminal Investigator/Special Agent with Internal Revenue Service - Criminal Investigative Division for approximately seven years. I've received training in child-pornography investigations, and I've had the chance to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I have received additional training from CETF and ICAC relating to online, undercover chatting investigations, as well as peer-2-peer or P2P investigations. While employed by HSI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. Specifically, I have participated in numerous investigations relating to the sexual exploitation of children over the Internet since 2013.

PURPOSE OF AFFIDAVIT

2. I submit this Affidavit in support of an application for a search warrant for a Samsung cell phone, bearing phone number 970-629-5231, that is currently secured in the Grand County Sheriff's Office in Moab, Utah under Case Number GCSO 2304793.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The facts in this affidavit are included based on my training and experience, as well as my review of reports written by other law enforcement officers.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18 U.S.C. §§ 2422(b)

(coercion and enticement of a minor) and 2423(b) (travel with intent to engage in illicit sexual conduct) have been committed by CODY WILLIAMS (the "Target Offenses). There is also probable cause to search the device described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of the Target Offenses as further described in Attachment B.

SEARCH METHODOLOGY TO BE EMPLOYED

5. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

c. surveying various file directories and the individual files they contain;

d. opening files in order to determine their contents;

e. using hash values to narrow the scope of what may be found. Hash values are used to find previously identified files of images of child pornography and do

not capture images that are the result of new production, images embedded in an alternative file format, or images altered, for instance, by a single pixel. Thus, hash value results are under-inclusive, but are still a helpful tool;

f. scanning storage areas;

g. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment A; and/or

h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

BACKGROUND REGARDING DIGITAL DEVICES

6. Based upon my training, my experience, and my discussions with other law enforcement agents, I know the following:

a. Users of digital devices increasingly choose to store items in digital form (e.g. pictures, documents) because digital data takes up less physical space, and can be easily organized and searched. Users also choose to store data in their digital devices, such as cell phones, because it is more convenient for them to access data in devices they own, rather than to later spend time searching for it. Keeping things in digital form can be safer because data can be easily copied and stored off site as a failsafe.

b. Users also increasingly store things in digital form because storage continues to become less expensive. Today, 500 gigabyte (GB) hard drives are not uncommon in computers. As a rule of thumb, users with 1 gigabyte of storage space can store the equivalent of 500,000 double spaced pages of text. Thus, each computer can easily

contain the equivalent of 250 million pages, that, if printed out, would fill three 35' x 35' x 10' rooms. Similarly, a 500 GB drive could contain 450 full run movies, or 450,000 songs, or two million images. With digital devices, users can store data for years at little or no cost.

c. Storing data in digital form and not deleting it mirrors users' online habits where users have, for years, been encouraged to never delete their E mails. For example, on March 27, 2007, Yahoo! Mail announced free, "unlimited" capacity that gave their users "the freedom to never worry about deleting old messages again." See < http://ycorpblog.com/2007/03/27/yahoo mail goes to infinity and beyond/> (accessed April 18, 2012). Similarly, since June 2007, Google, Inc. has promoted free, increasingly larger storage "so you should never have to delete mail." <http://gmailblog.blogspot.com/#!/2007/06/welcome to official gmail blog.html>; see also <http://gmailblog.blogspot.com/2007/10/more gmail storage coming for all.html> (accessed April 18, 2012) (promoting its "Infinity+1" plan to constantly give subscribers more storage). Hotmail also has advertised free, "virtually unlimited space," noting that "Hotmail gives you all the space you need." See <http://www.microsoft.com/windows/windowslive/anotherlookathotmail/storage/> (accessed April 18, 2012).

d. Digital devices can also store data automatically, without a user's input. For example, network logs may track an employee's actions for company auditing purposes or E mail headers may automatically list the servers which transmitted the E mail. Similarly, a web browser (i.e. an application such as Internet Explorer used to access web

pages) can track a user's history of websites visited so users can more easily re access those sites. Browsers also often temporarily cache files from recently accessed web pages to improve the user's experience by reducing that page's loading time. These examples illustrate how the interaction between software and operating systems often results in data being stored without a user's knowledge. Even if a sophisticated user understands this automatic storage of data, attempts at deleting this data often fail because the data may be automatically stored multiple times and in different locations. Thus, digital evidence may exist despite attempts at deleting it.

e. Digital data is particularly resilient to deletion. First, as noted, data is often automatically stored multiple times in multiple places, where even sophisticated users may not be able to locate. Second, digital data can be recovered years after it has been saved, or viewed B even after such data has been deleted. For example, when a user deletes a file on a computer, the file is sent to the recycle bin, where it can still be retrieved. Even if the file is deleted from the recycle bin, the data does not actually disappear; rather, it remains in "free space" or "slack space" (i.e. in unused space) until it is overwritten by new data. Third, an operating system may also keep deleted data in a "recovery" or "swap" file. Fourth, files from websites are automatically retained in a temporary cache, which are only overwritten as they are replaced with more recently viewed web pages. Thus, the ability to retrieve residues of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer use habits.

///

DETAILS OF THE INVESTIGATION

7. On May 14, 2023, an undercover officer with the Grand County Sherriff's Office (GCSO) had an account on MeetMe, a web-based social media application. On the account, the undercover officer listed her age as 27. On that date, a person with the account name "Cody" contacted the undercover profile and the UC asked if he wanted to text. "Cody" then sent a text to the UC on May 16 from phone number **970-629-5231** and the two then began exchanging text messages. The UC told "Cody" her name was "Ash."

8. Very early in the conversation on May 16, and before any sexual messages were exchanged, "Cody" asked the UC what she was doing and she responded that she "just got out from school." When "Cody" asked the UC if she was referring to college, the UC replied that she was in middle school and told "Cody" she was 13 "but I've been told I look and act older tho." "Cody" then asked why she was on MeetMe and the UC said she was curious about boys and the two continued exchanging messages. "Cody" then asked the UC what she looked like and the UC sent an age-regressed photo that approximated a 13-year-old girl; "Cody" responded "cute." When the UC said she wished she was older, "Cody" responded that he wished he was younger because "One I wouldn't get into trouble talking to you," and said he could get in trouble "Because of the age difference if we talk different." The UC responded that she wouldn't tell and then asked "Cody" for a photo. "Cody" sent a selfie-style photo depicting the face of an adult male with sunglasses and a beard. The UC replied "cute."

9. "Cody" then asked the UC what she was thinking about and the UC responded that she was hungry. "Cody" replied "I could say something so dirty lol." When

the UC asked him what he meant, "Cody" replied "you said you was hungry I got something to feed you." When the UC asked him what he would feed her, "Cody" said "I can't say" and asked her to guess. The UC then sent an eggplant emoji and "Cody" responded "ding." The UC then expressed embarrassment and nervousness because she doesn't "know a lot" and "Cody" replied that he would help her learn.

10. On May 17, the text messages continued. "Cody" asked what the UC was doing and she said she was eating breakfast. "Cody" then replied "Can I eat you." "Cody" then apologized and said he "shouldn't talk to you like that." The two then continued to exchange sexual messages discussing what "Cody" could "teach" the UC. He asked if the UC had ever "played with herself" and asked her what she was wearing. "Cody" also admitted that he "played" with himself and was nude at the time. The two then began discussing "Cody" performing oral sex on the UC when he asked "do you know what getting ate out is," and elaborated he would lick "inside around all over." "Cody" then asked if he could see a photograph of the UC's vagina and offered "I wouldn't send it to anyone I'd delete it."

11. On May 18, the sexual messages between the UC and "Cody" continued. The UC told "Cody" "you don't have to talk to me if my age freaks you out" and "Cody" responded "no I just don't want to get in trouble" and asked the UC to delete everything and not tell anyone about their messages. The two then discussed whether "Cody" had a girlfriend and he asked the UC if she wanted to be his girlfriend; the UC agreed to be his "secret girlfriend."

12. On May 19, the two continued exchanging messages and "Cody" told the UC that he was 28 years old and again repeated that the UC needed to "hide our tracks." The UC again stated "we can stop talking if you want" but "Cody" insisted it was "fine." The two also continued messaging on May 20.

13. On May 21, "Cody" asked the UC "let me ask do you want to learn just basic kinky hard core what." He then explained "so basic is kissing touching undressing blow job me licking your pussy," and "kinky is ill lick you from your pussy to your ass fingering your ass and pussy and you suck my cock lick my ass fart on my cock stuff like that." "Cody" admitted he liked "kinky," and the UC offered to learn. Later that day, "Cody" sent the UC links to two adult pornography websites and told her to watch some videos.

14. On May 22, the two began discussing meeting during the upcoming weekend. The UC said she would be in Thompson Springs, Utah, which was relatively close to Grand Junction, Colorado where "Cody" said he lived. The two talked about what they would do when they met and the UC offered "we can try that kinky stuff u sad." Ultimately, "Cody" said he was unable to come meet the UC that weekend and the UC responded "it's ok if u dnt want to. U don't have to."

15. Between May 23 and June 14, the two continued to exchange messages discussing the difficulty of long-term relationships and when they may be able to see each other in person. "Cody" said he was working a lot at an oil field where he was employed and was having trouble getting time off to come visit the UC. On June 14, the UC told "Cody" that she missed him and "Cody" asked the UC to show him how much she missed him, messaging "show daddy now make daddy want to cum." The UC again declined to

send any nude photos until the two met in person and once again reiterated "u don't have to cum u dnt even have to talk to me." "Cody" confirmed that he wanted to be with the UC and that he loved her.

16. On June 15, the UC asked "r u cuming this wknd or not" and again reiterated that he didn't have to; "Cody" replied "I'm going to try yes." On June 16, the two discussed whether "Cody" needed to bring condoms. The UC said she didn't have any and "Cody" asked "what if I pull out" or if they could have anal sex. "Cody" promised he would "cum" wherever the UC wanted "in your pussy ass mouth wherever you want just tell me." "Cody" committed to driving to Thompson Springs, Utah, the next morning.

17. On June 16, "Cody" asked if he got the UC "the pill" whether she would let him ejaculate inside her. Later that morning, "Cody" asked the UC "wanna fart on my cock." "Cody" confirmed that he would arrive in Thompson Springs at around 8:30 AM. He later said he was "5 miles away."

18. During the course of these messages, law enforcement were able to identify "Cody" as Cody WILLIAMS. On June 16, police officers established surveillance at WILLIAMS' known residence and identified WILLIAMS as he walked to his truck at approximately 7:15 AM. Officers then observed WILLIAMS walk inside his residence for a short period before walking back to his truck around 7:30 AM and driving toward Thompson Springs. Officers then followed WILLIAMS from Grand Junction to Thompson Springs and his physical travel was consistent with updates "Cody" provided to the UC via text message. WILLIAMS then pulled into a gas station at Thompson Springs where "Cody" and the UC agreed to meet. As WILLIAMS parked his truck, officers approached

and took him into custody without any issue. As he was being arrested, WILLIAMS spontaneously stated he was on his way to Salt Lake City. After WILLIAMS' arrest, the UC sent a confirmatory text to "Cody" and the Samsung phone found in WILLIAMS' truck received the text (the "**Subject Device**").

19. Officers secured a State search warrant for the Subject Device and executed it. The results of that search warrant are not being relied upon for purposes of this warrant.

CONCLUSION

20. Based on the facts set forth in this affidavit, I respectfully submit that there is probable cause to believe that the Subject Device contains evidence of coercion and enticement of a minor as well as travel with intent to engage in illicit sexual conduct in violation of Title 18, United States Code, Sections 2422(b) and 2423(b) and that the information sought herein will materially aid the investigation.

RESPECTFULLY SUBMITTED this 29th day of September, 2023.

IVAN J MURRAY Digitally signed by IVAN J MURRAY
Date: 2023.09.29 08:10:34 -06'00'

Ivan Murray, Special Agent
Homeland Security Investigations

Subscribed and sworn to before me this _____ day of September, 2023.

JUDGE PAUL KOHLER
United States Magistrate Judge

ATTACHMENT "A"

Property to Be Searched

The Subject Device is described as a Samsung cell phone, bearing phone number 970-629-5231, and any SIM card contained therein, that is currently secured at the Grand County Sheriff's Office in Moab, Utah under Case Number GCSO 2304793.

ATTACHMENT B
LIST OF ITEMS TO BE SEARCHED FOR AND SEIZED

This affidavit is in support of application for a warrant to search a Samsung cell phone bearing phone number 970-629-5231, and any SIM card contained therein, which is more specifically identified in the body of the application and in Attachment A ("Subject Device"), that can be used to store information and/or connect to the Internet, or which may contain mobile devices, for records and materials that are fruits, evidence, or instrumentalities of violations of Title 18, United States Code, Sections 2422(b) and 2423(b). These records and materials are more specifically identified as:

1. Any and all computer software, including programs to run operating systems, applications (like word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs;

2. Any computer-related documentation, which consists of written, recorded, printed or electronically stored material that explains or illustrates how to configure or use computer hardware, software or other related items;

3. Any and all records and materials, in any format and media (including, but not limited to, text messages, SMS messages, picture/video messages, social media communication, envelopes, letters, papers, e-mail, chat logs and electronic messages), pertaining to the Target Offenses;

4. Any evidence relating to any MeetMe profile accounts accessed by the Subject Device;

5. Records and information evidencing occupancy or ownership of the Subject

Device described above, including, but not limited to, sales receipts, registration records, records of payment for Internet access, usernames, passwords, device names, and records of payment for access to newsgroups or other online subscription services;

6. Stored electronic data and related digital storage relating to Global Positioning System ("GPS") data;

7. Records evidencing the use of the Subject Device's capability to access the Internet, including: records of Internet Protocol addresses used and records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

8. Images and videos, to include any metadata identifying the date and location of the Subject Device at the time of the photo or video pertaining to the Target Offenses;

9. Evidence of who used, owned, or controlled the Subject Device at the time the things described in this warrant were possessed, accessed, received, created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

10. Evidence of software that would allow others to control the Subject Device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software; and evidence of the lack of such malicious software;

11. Evidence of counter-forensic programs (and associated data) that are designed

to eliminate data from the Subject Device;

12. Evidence of the times the Subject Device was used;

13. Passwords, encryption keys, and other access devices that may be necessary to access the Subject Device.